Chapter 50

Trustee-based Tracing Extensions to Anonymous Cash and the Making of Anonymous Change

Ernie Brickell* Peter Gemmell* David Kravitz*

Abstract

Electronic cash is a subject of great economic, political, and research importance. With advances in computer networks, in processor speed, and in databases and with advances in note counterfeiting technology and with both individuals' and businesses' desire for remote and more convenient financial transactions, some forms of electronic cash are likely to become widespread within 5 to 10 years. While unconditionally anonymous electronic cash systems have been proposed in the literature, governmental and financial institutions are unwilling to back a completely anonymous system. Instead, they have proposed systems with little or no protection for the users' privacy. Their reasons for opposing complete untraceability have to do with the containment of user fraud and the desire to restrict the new kinds of crime that unrestricted remotely withdrawable and spendable electronic cash could facilitate.

We introduce the first electronic cash systems which incorporate *trustee-based tracing* but otherwise provably protect user anonymity. We expand on the provably anonymous electronic cash systems of [B93] and [FY92]. Our systems maintain the previous papers' complete provable user anonymity except that, only with the cooperation of several publicly appointed trustees (key-escrow agents), the government can trace a user's spending with certainty, determining to whom the user gave his/her money and how much s/he gave. The trustees can answer the question of whether a particular payment was made by a particular user, without revealing any additional information. This allows for authorized forward and backward tracing that does not impinge on the privacy of anyone other than the parties of the one transaction in question. The trustee-based tracing requires no tamper-resistant hardware and can be implemented as either on-line or off-line systems.

For those concerned about the trustability of the trustees, we describe how a mutually distrustful government and user can construct an *electronic trustee*, a device which can be used in place of (or in addition to) ordinary human trustees. This device, which does use tamper-resistant and tamper-detecting hardware, automatically alerts the user in case his/her secret stored by the trustee is released or compromised.

Furthermore, we introduce an on-line *anonymous change-making* protocol that is independent of trustee-based tracing. This protocol addresses a major stumbling block for anonymous cash systems: how a user can make an anonymous purchase at a store when the user does not have correct change. We are able to provide exact, perfectly anonymous change, assuming a line of communication with a coin-minting facility. There is no need to determine on-line that the user's coins have not been spent before.

*Sandia National Labs, MS 1110, PO Box 5800, Albuquerque, NM 87185-1110. E-mail Contact: psgemme@cs.sandia.gov.
This work was performed at Sandia National Laboratories and was supported by the U.S. Department of Energy under contract DE-AC04-76DP00789.

1 Introduction

We present electronic cash systems that we believe can be put into practice. Our systems have the following properties:

- The systems are reasonably acceptable to users who are concerned about invasion of their privacy.

  We envision that each individual is allowed to withdraw remotely a modest amount of completely untraceable electronic cash, say about $100, per day. Other completely untraceable cash would be withdrawn in-person from such places as an ATM or from a bank branch.

- The systems are acceptable from the point of view of law enforcement and crime prevention.

  Aside from the completely untraceable money, each individual is allowed to withdraw remotely as much money as s/he has, from any location, in the form of *trustee-traceable* electronic cash. This means that if law enforcement gets the trustees' approval, it can get from the trustees information to determine where a user has spent his/her trustee-traceable money.

  While it is possible for trustee-based systems to have an arbitrary number of trustees and for the trustee-based tracing to have an arbitrary positive access structure associated with it, for the sake of simplicity, the systems which we present in this extended abstract have two trustees, both of whom are required for a trace to be effective.

  The trustee-based tracing can be accomplished completely through cryptology and has no need for tamper-resistant hardware. It works as follows:

  When the user sets up his/her bank account, the user provides the trustees collective information which later would allow them to recognize the user's trustee-traceable coins. If a trace is ordered by the courts or authorized by the user, the trustees use their information to recognize payments involving the user's money. This technique is described in section 3.

- The systems address the major problem of the user trying to make a purchase without correct change

while maintaining (either unconditional or trustee-based) user anonymity. Our anonymous change-making protocol is on-line, in the sense that it requires that the user must be able to communicate anonymously with an electronic coin-minting facility. However, unlike the solutions proposed in [Cha89], there is no need for the system to check, during the change-making transaction, that the user's coins have not been spent already. Our protocol is independent of trustee-based tracing and can be used in either the context of a completely anonymous system or a trustee-based system.

A privacy-minded user does not want to accept coins from a store as change because those coins might be traceable in a way not obvious to the user. Also, the user does not want to identify him/herself to the bank immediately before making the purchase because the bank could then associate the user with the store. The bank might make this association either by learning the user's physical location at the store via the user's communications or observing that the change-making happens close to the time that the store deposits the money the user gave it. Our protocol allows a user desiring correct change, but not wishing to reveal his/her identity to the bank, to exchange anonymously one set of coins for another set of coins of equal total value, but different denominations. The bank does not learn the user's identity, but the system's protection against multiple-spending of electronic money and other fraud remains intact.

Furthermore, we note that no off-line, perfectly unlinkable, and efficient cash-divisibility scheme is possible. This is so in the following sense: if all the pieces of a divisible coin are information-theoretically unlinkable, then the total entropy of the coin (and the number of bits associated with the coin) must be proportional to the maximum number of legitimately spendable pieces. Therefore, the only hope for creating unlinkable divisible coins is to put the user's privacy in terms of complexity assumptions.

The security and privacy properties of our protocol are based on the algebraic properties of a large subgroup of prime order q embedded in the multiplicative group Z_p^*, where p is a large prime.

- The systems are secure against counterfeiting and other fraud. We present one version of the system based on [B93], where the security is based on the existence of a collision-free hash function and the difficulty of finding discrete logarithms, and one version based on [FY92], where the security is based on the existence of a collision-free hash function and the difficulty of factoring as well as the difficulty of finding the discrete log.
- The systems protect the user against false charges of spending electronic money. Even with the help of all the trustees, the government can not feasibly make the user appear to have made a payment s/he did not make.
- The systems allow for the transferability of coins as described in [vA90] and [CP92]. Furthermore, the transfers can be made trustee-traceable.

1.1 Previous Work.

There is a great amount of literature on electronic cash. Previously proposed systems can be divided into two types:

- Those that offer little privacy for the users of the system. These systems either neglect the privacy issue altogether or trust the banks, the government, or other central authority not to pry into users' financial dealings.
- Privacy-protecting systems. These tend to be more difficult to design because they have to prevent the bank from learning too much about the user while still giving the bank power to prevent or detect fraud by the user. Most such systems use a concept called *blind signatures* which is due to Chaum [Cha83]. A blind signature scheme is a protocol in which the signer (the bank or the mint) signs a piece of information for the recipient (the electronic cash system user) without being aware of exactly which signature it is providing. The recipient obtains a signature but does not learn anything from the protocol which would enable him or her to sign other things. This type of signature scheme, when used in the context of electronic cash, enables the user to withdraw money from the bank, spend it at a store, and be confident that when the store deposits the money at the bank, the bank will not be able to recognize the money as the same cash given to the user. [CFN90], [OO92], [FY92], and [B93] are examples of systems which employ blind signatures.

  So far, there are two basic blind signature schemes, one due to Chaum and Pedersen [CP93] and the other due to Chaum ([Cha85] and [Cha88]).

  [Cha85] and [Cha88] introduce a protocol based on the difficulty of computing cube roots modulo an RSA modulus N with unknown factorization. The idea is that the bank knows the factorization of the modulus and is able to compute pairs

$(y, \mathcal{H}(y)^{1/3} \bmod N)$ where $\mathcal{H}$ is a collision-free hash function. The user chooses random $x, r \bmod N$ and sends $r^3\mathcal{H}(x) \bmod N$ to the bank. The bank sends $r\mathcal{H}(x)^{1/3}$ to the user who extracts the coin $(x, \mathcal{H}(x)^{1/3})$ which is unknown to the bank.

[CP93] introduces a protocol based on the difficulty of computing the discrete log of a number h mod p where p is a large prime. The bank sets $h = g^x \bmod p$ where g is a public generator. The bank then publicizes h but keeps x secret. The blind signature scheme is somewhat complicated and is presented as part of the protocols of subsection 3.2.

Two previous techniques to deal with the problem of providing change anonymously are due to Ohta and Okamoto [OO92] and Eng and Okamoto [EO94] who developed protocols which enable a user to split his or her coins into pieces and give different stores different pieces. The trouble with their solution is that, while the bank may not know who withdrew the coin, the bank will recognize the different pieces as belonging to the same coin. Thus, the pieces are linkable.

1.2 Privacy, Kidnapping, Extortion, Lost Money, and other Issues.

Due to space considerations, we defer the bulk of our discussion of these important but less technical issues to the full paper. One problem with previously proposed privacy-preserving electronic cash systems is that they make kidnapping and other forms of extortion more viable than with paper-based transactions (see [vSN92]).

1.3 Organization of the Paper.

In section 2, we define terms.

In subsections 3.2 and 3.3, respectively, we incorporate trustee-traceability into two previously published cash transaction systems.

In section 4, we describe an electronic trustee which automatically alerts the user when s/he is being traced.

In section 5, we present our solution to the problem of making a completely anonymous purchase when the user does not have correct change.

2 Definitions

We define terms that we'll use throughout the rest of the extended abstract.

- $\mathcal{U}$, the User or the User's card: The User is anyone who withdraws and spends electronic money. The User's card is a card constructed for and trusted by the user. It is the device with which s/he makes withdrawals, purchases, and reports transactions. $\mathcal{ID}_{\mathcal{U}}$ is a user ID which is associated with $\mathcal{U}$.
- $\mathcal{B}$, the Bank: An institution which dispenses electronic cash for withdrawal and accepts it for deposit. The bank should not have the power to trace users' spending.
- Trustee: A person or device that stores part of a secret which can be used to trace the user's financial transactions.
- G, the Government: A regulator of the financial system. G should only be able to trace the users' money if G has the trustees' cooperation.
- $\mathcal{H}$: A collision-free hash function.

3 Incorporating Trustee-based Tracing into the Cash Protocols

We present means by which trustee-based tracing is directly incorporated into the basic electronic cash protocols of Brands and Franklin-Yung. The tracing mechanism is efficient and the user's card needs to converse with trustees only upon the set-up of his/her account. Furthermore, the trustee-based tracing requires no tamper-resistant hardware and, as long as the trustees do not cooperate in an attempt to trace the user's spending, the system preserves the security and complete anonymity of the original anonymous cash schemes.

We note here that in the above-described systems, an answer to the question of where a user spent one of his/her electronic coins would involve a binary search over a potentially very large database of deposits. While they also have the advantage that they do not require tamper-resistant hardware and while they provide for the cryptographic tracing of double-spenders, we believe that any acceptable general use offline system must *prevent* double-spending and that this will involve stationing a tamper-resistant device in the user's electronic wallet.

In the full paper, we consider a method of trustee-based tracing that is centered on a tamper-resistant observer. This has the advantage that there is no need for legitimate traces to access large databases.

In the full paper, we describe two extensions that allow for the tracing of a user's financial transactions by trustees. Both of these extensions are centered around having the user send an encrypted version of his or her transaction records periodically to an *Automatic Records Deposit Machine* ($\mathcal{ARDM}$). The records are encrypted in such a way that it would require both trustees to decrypt them. The deposits of the records may be done remotely.

The first, more simple, extension is based on the idea that the user's wallet will be fabricated in a facility trusted by both the user and the government.

In the second extension, there is no single device which is trusted by both the user and the government. Instead, the user builds his/her own card and the tamper-resistant government-trusted observer is stationed within it.

3.1 Proving Combined Knowledge of a Representation.

At various times in the protocols of subsection 3.2 and 3.3, the trustees, T_1 and T_2, will wish to show a third party (a verifier) that they have combined knowledge of a representation of some number h relative to generators g_1, g_2.

Proving Combined Knowledge of a Representation

P_1 and P_2 claim to have combined knowledge of a representation of h is terms of g_1, g_2.
P_1 knows $g_1^{a_{1,1}} g_2^{a_{1,2}}$. P_2 knows $g_1^{a_{2,1}} g_2^{a_{2,2}}$.
P_1 proves knowledge of a representation of $g_1^{a_{1,1}} g_2^{a_{1,2}}$ to V.
P_2 proves knowledge of a representation of $g_1^{a_{2,1}} g_2^{a_{2,2}}$ to V.
V checks that $h = (g_1^{a_{1,1}} g_2^{a_{1,2}}) g_1^{a_{2,1}} g_2^{a_{2,2}}$

The following protocol appears in [B93]:

Proving Knowledge of a Representation

(P knows $y = g_1^{a_1} g_2^{a_2}$.)
P: compute $w_1, w_2 \in_R Z_q$, $z = g_1^{w_1} g_2^{w_2}$.
send $z, (g_1, g_2), y \longrightarrow V$.
V: send challenge $c \in_R Z_q \longrightarrow P$.
P: send $r_i = w_i + ca_i \bmod(q)$ for $i = 1, 2 \longrightarrow V$
V: check $zy^c = g_1^{r_1} g_2^{r_2}$.

3.2 Incorporating Trustee-based Tracing into Brands' Protocols.

We describe a modification of Brands' protocols which allows for trustee-based tracing. There is no need for any tamper-resistant devices or any inconvenience to the user. The security of all parties is based only on cryptographic assumptions. The trustees participate in an interactive process during the account $Set - Up$ protocol, when they conduct proofs of knowledge of a representation for each value f_k (k indexes the coin withdrawn by the user and each coin has a different value f_k).

Let p, q be large primes such that $q|(p-1)$ and let $\mathcal{G} \subset Z_p^*$ be the subgroup of order q. Let g, g_1, g_2, g_3, g_4, d be generators of $\mathcal{G}$ randomly chosen by the bank.

The values $h_i = g^{\alpha_i}$ are information published by the bank for verifying the authenticity of the electronic coins, where the index i refers to the coin's denomination. Knowledge of α_i allows the bank to mint coins of denomination i.

The set-up, withdrawal, and payment protocols are extensions of Brands' basic set-up, withdrawal and payment protocols.

In the new set-up protocol, the user gives the trustees information which would allow them to link any payment involving each coin to its withdrawal. This information is the combined knowledge of $\mathcal{U}$'s representation of the value $f_k = g_3^{\gamma_{3,k}} g_4^{\gamma_{4,k}}$. The trustees prove to the government that they know a representation for f_k.

Set-Up-With-Trustees

$\mathcal{U}$: generate random u_1, u_2 and send $I_{\mathcal{U}} = g_1^{u_1} g_2^{u_2} \longrightarrow \mathcal{B}$.
$\mathcal{B}$: associate $I_{\mathcal{U}}$ with $\mathcal{U}$'s identity, $\mathcal{ID}_{\mathcal{U}}$, choose random α_i for each coin denomination i and broadcast $g, h_i = g^{\alpha_i}$.
Let N be an upper bound on the number of coins which $\mathcal{U}$ will withdraw.
$\mathcal{U}$: choose $\{\gamma_{3,k}, \gamma_{4,k}\}_{k=1}^{N} \in_r Z_q$.
For each k, randomly split
$\gamma_{3,k} = s_{1,1}^k + s_{2,1}^k, \gamma_{4,k} = s_{1,2}^k + s_{2,2}^k \bmod (q)$
send $s_{1,1}^k, s_{1,2}^k \longrightarrow T_1$, $s_{2,1}^k, s_{2,2}^k \longrightarrow T_2$.
For each k, send $f_k = g_3^{\gamma_{3,k}} g_4^{\gamma_{4,k}} \longrightarrow \mathcal{B}$.
For each k, trustees T_1 and T_2 prove combined knowledge of a representation of f_k to $\mathcal{B}$ relative to g_3 and g_4.

The new withdrawal protocol is very similar to the protocol of [B93] except that $m = I_{\mathcal{U}} d f_k$.

The underlying idea of Brand's protocol is that $\mathcal{B}$ provides $\mathcal{U}$ with a blind signature that is a tuple (A, B, z', a', b', r'). This tuple satisfies the equations $g^r = h^{\mathcal{H}(m',z',a',b',A)} a' \bmod(p)$ and $m'^{r'} = z'^{\mathcal{H}(m',z',a',b',A)} b' \bmod(p)$. If $\mathcal{H}$ is a collision-free hash function, it is believed to be hard to create a tuple of this form without finding the discrete log of h (see [B93]). Furthermore, because the signature is blinded, the tuple is uniformly distributed among all such tuples when one is given only the bank's view of the conversation.

Withdrawal-With-Trustees(for denom. i) (for $\mathcal{U}$'s kth withdrawal). Let $h = h_i, \alpha = \alpha_i$.

$\mathcal{U}$: prove knowledge of a representation of $I_\mathcal{U} = g_1^{u_1} g_2^{u_2} \bmod(p)$ to $\mathcal{B}$

$\mathcal{B}$: choose $w \in_R Z_q$ and set $m = I_\mathcal{U} d f_k$.
send $z = m^\alpha, a = g^w, b = m^w \longrightarrow \mathcal{U}$.

$\mathcal{U}$: choose $s \in_R Z_q^*$, set $m' = m^s, z' = z^s$,
choose $x_1, x_2, x_4, x_5 \in_R Z_q$, set
$y_1 = u_1 s - x_1, y_2 = u_2 s - x_2 \bmod(q)$,
$y_4 = \gamma_{4,k} s - x_3, y_5 = s - x_5 \bmod(q)$,
let $A = g_1^{x_1} g_2^{x_2} g_3^{\gamma_{3,k} s} g_4^{x_4} d^{x_5}$,
$B = g_1^{y_1} g_2^{y_2} g_4^{y_4} d^{y_5}$
choose $u, v \in_R Z_q^*$, set $a' = a^u g^v$,
$b' = b^{su} (m')^v$, $c' = \mathcal{H}(m', z', a', b', A)$,
send $c = c'/u \longrightarrow \mathcal{B}$.

$\mathcal{B}$: send $r = \alpha c + w \bmod(q) \longrightarrow \mathcal{U}$.

$\mathcal{U}$: verify $g^r = h^c a, m^r = z^c b \bmod(p)$,
set $r' = ru + v \bmod(p)$,
set. $sign_\mathcal{B}(A, B) = (z', a', b', r')$.

In the new payment protocol, the user is forced to reveal the value $r_3 = \gamma_{3,k} s$. Later, if the trustees give the government the value $\gamma_{3,k}$ from the execution of the withdrawal protocol and the government has the values $m', r_3 = \gamma_{3,k} s$ from an execution of a payment protocol, then the government can compute s and $I_\mathcal{U} d = m'^{s^{-1}} / f_k \bmod (p)$, thereby linking the payment with the withdrawal.

Payment-With-Trustees

$\mathcal{U}$: send $A, B, sign_\mathcal{B}(A, B) = (z', a', b', r')$,
$r_3 = \gamma_{3,k} s \bmod(q) \longrightarrow \mathcal{S}$.

$\mathcal{S}$: verify that $AB \neq 1$, verify $sign_\mathcal{B}(A, B)$,
send $c_1 = \mathcal{H}(\mathcal{ID}_\mathcal{S}, time, r_3, A, B) \longrightarrow \mathcal{U}$.

$\mathcal{U}$: send $r_1 = x_1 + c_1 y_1 \bmod(q), r_2 = x_2 + c_1 y_2$,
$r_4 = x_4 + c_1 y_4, r_5 = x_5 + c_1 y_5 \longrightarrow \mathcal{S}$.

$\mathcal{S}$: verify $g_1^{r_1} g_2^{r_2} g_3^{r_3} g_4^{r_4} d^{r_5} = AB^{c_1} \bmod(p)$.

In the deposit protocol, the store $\mathcal{S}$ sends a transcript of the payment protocol to both the bank $\mathcal{B}$ and the government G.

The procedure which the government can use to trace multiple spenders is the same as that in Brands' basic protocols and included here for completeness.

Tracing Multiple Spenders

The bank $\mathcal{B}$ has records of a coin spent two times, with two different challenges, β, β'.

To identify the user, $\mathcal{B}$ uses the two sets of responses (r_1, r_2, r_3) and (r_1', r_2', r_3').

$\mathcal{B}$: compute $z_2 = \frac{r_3 - r_3'}{\beta - \beta'}, z_1 = r_3 - \beta z_2, s = z_1 + z_2$,
$x_2 = \frac{r_1 - r_1'}{\beta - \beta'}, x_1 = r_1 - \beta x_2, u_1 = x_1 + x_2$,
$y_2 = \frac{r_2 - r_2'}{\beta - \beta'}, y_1 = r_2 - \beta y_2, u_2 = y_1 + y_2, I_\mathcal{U} = g_1^{u_1} g_2^{u_2}$.

When presented with a court order, the trustees will provide the government means to trace user $\mathcal{U}$.

In the second protocol, the trustees don't give the government the value $\gamma_{3,k}$. Instead, they determine only whether $m'^{r_3^{-1}} = (I_\mathcal{U} d f_k)^{\gamma_{3,k}^{-1}}$ by attempting to prove knowledge of a representation of $I_\mathcal{U} d f_k$ in terms of the single generator $m'^{r_3^{-1}}$.

Trace-With-Trustees

Government G: ask T_1 and T_2 for all sets of withdrawal values $\{s_{i,j}\}_{i,j \in \{1,2\}}$ for user $\mathcal{U}$.
For all withdrawals, compute
$\gamma_{3,k} = s_{1,1} + s_{1,2} \bmod (q)$
Search the database of payment transcripts for $m'^{r_3^{-1}} = (I_\mathcal{U} d f_k)^{\gamma_{3,k}^{-1}}$.
If so, that is $\mathcal{U}$'s coin.

Trace-One-Payment

The government G wants to know whether a particular payment was made by a user $\mathcal{U}$.

Let $\{s_{i,j}^k\}_{i=1,2; j=1,2, k=1 \ldots N}$ be the shares given by $\mathcal{U}$ to T_1 and T_2 during the user's N executions of the withdrawal protocol.

G: obtain a court signature for the payment in question.
send $m', r_3, I_\mathcal{U}, sign_\mathcal{C}(m', r_3, I_\mathcal{U}) \longrightarrow T_1$ and T_2.

T_1 and T_2: For each value, f_k, attempt to prove combined knowledge of a representation of $I_\mathcal{U} d f_k$ relative to $m'^{(r_3^{-1} \bmod (q))}$, using their knowledge of $s_{1,1}^k$ and $s_{1,2}^k$

G: If T_1 and T_2 succeed, assumes that the coin involving m' was spent by $\mathcal{U}$.

LEMMA 3.1. *The above protocols satisfy the following properties:*

1. *They preserve the protections of [B93] against counterfeiting and multiple spending.*
2. *The values A, B, z', a', b', r', $r_1, r_2, r_3, r_4, r_5, c$ appearing in the payments of a user's coins are completely independent from the values $I_\mathcal{U}, f_k, w, m$,*

z, a, b, c, r, (and the values appearing in the trustees' proof of knowledge of a representation of f_k) appearing in the user's withdrawals. Therefore, without help from all the trustees, the user's cash is information-theoretically anonymous.

3. *If the user can not forge Schnorr signatures and if the hash function, $\mathcal{H}$, is designed correctly, then it is infeasible for the user to prevent the trustees from linking his/her withdrawals to his/her payments.*

4. *If the user does not reveal the representation $I_{\mathcal{U}} = g_1^{u_1} g_2^{u_2}$, then the government, even with the help of all the trustees, could successfully claim that an honest user made a payment s/he did not make only if the government or the trustees can compute discrete logs.*

5. *If there is a legitimate payment such that an honest government G is able to link withdrawals from both user $\mathcal{U}$ and user $\hat{\mathcal{U}}$ to that payment, then $\mathcal{U}$ and $\hat{\mathcal{U}}$ can combine their information to get a non-trivial representation of 1 relative to generators g_1, g_2, g_4, d. This means that dishonest users cannot create false links between withdrawals and payments.*

See Appendix A for the proof.

3.3 Incorporating Trustee-based Tracing into the Franklin And Yung-type Protocols.

The trustee-based tracing relies on the user encoding information to unlock the secrets of his/her coin in the coin released during the withdrawal protocol. This information is encoded using public keys E_1, E_2, whose private key counterparts are known to trustees T_1 and T_2 respectively.

Let $\mathcal{U}$ be the user, S be a shop, $\mathcal{B}$ be the bank, G be the government, and T_1, T_2 be trustees. T_1 knows private key Θ_1 and publicizes public key E_1. T_2 knows private key Θ_2 and publicizes public key E_2. Let $\Theta = \Theta_1 \odot \Theta_2$. $\mathcal{B}$ and G know the factorization $n = q_1 q_2$.

Set-Up-With-Trustees
$\mathcal{B}$: publish large primes p, q such that
q divides $p-1$, $g \in Z_p^*$ of order q, and
an RSA modulus n whose factors $\mathcal{B}$ knows

The withdrawal protocol employs a technique called "cut and choose." In the process of acquiring an electronic coin, the user presents k randomized tuples to the bank. The bank selects $k/2$ of these tuples randomly and asks the user to show that they are properly constructed. The remaining $\frac{k}{2}$ tuples are used to create the coin. For each tuple, the user provides information that would allow for a trace. If the user cooperates on at leat 3/4 of the tuples, a trace can be done.

Withdrawal-With-Trustees
$\mathcal{U}$: prove identity to $\mathcal{B}$ (and sign all subsequent messages), choose k tuples
$(r_i, a_{1i}, a_{2i} = \mathcal{ID}_{\mathcal{U}}/a_{1i} \bmod(q),$
$E_1(u_{1i}, u_{2i}), E_2(v_{1i}, v_{2i}))$
where for $i \in [1 \ldots k]$, $r_i \in_R Z_p^*, u_{1i}, u_{2i} \in_R Z_q$
and $u_{1i} + v_{1i} = a_{1i}$, $u_{2i} + v_{2i} = a_{2i}$,
send $\{r_i^3 \mathcal{H}(g^{a_{1i}} \bmod(p) || g^{a_{2i}} \bmod(p)) \bmod(n);$
$E_1(u_{1i}, u_{2i}), E_2(v_{1i}, v_{2i})\}_{i=1}^{k} \longrightarrow \mathcal{B}$.
$\mathcal{B}$: send $L \subset \{1 \ldots k\}, |L| = \frac{k}{2} \longrightarrow \mathcal{U}$.
$\mathcal{U}$: send $\{(r_i, a_{1i}, a_{2i}, u_{1i}, u_{2i}, v_{1i}, v_{2i})\}_{i \in L} \longrightarrow \mathcal{B}$.
$\mathcal{B}$: For all $i \in L$, $j = 1, 2$, verify that
$\mathcal{ID}_{\mathcal{U}} = a_{1i} a_{2i}, a_{ji} = u_{ji} + v_{ji}$, verify that
$\{r_i^3 \mathcal{H}(g^{a_{1i}} \bmod(p) || g^{a_{2i}} \bmod(p)) \bmod(n);$
$E_1(u_{1i}, u_{2i}), E_2(v_{1i}, v_{2i})\}_{i \in L}$
is formed correctly, and send
$\Pi_{i \in \overline{L}} (r_i^3 \mathcal{H}(g^{a_{1i}} \bmod(p) || g^{a_{2i}} \bmod(p)))^{\frac{1}{3}} \bmod(n)$
$\longrightarrow \mathcal{U}$
$\mathcal{U}$: compute
$\Pi_{i \in \overline{L}} (\mathcal{H}(g^{a_{1i}} \bmod(p) || g^{a_{2i}} \bmod(p)))^{\frac{1}{3}} \bmod(n)$

Payment-With-Trustees
$\mathcal{U}$ wants to spend a coin at C shop S:
$C = \Pi_{i \in \overline{L}} (\mathcal{H}(g^{a_{1i}} \bmod(p) || g^{a_{2i}} \bmod(p)))^{1/3} \bmod(n),$
$\{x = (\mathcal{ID}_S || time)\},$
$\{g^{a_{1i}} \bmod(p), g^{a_{2i}} \bmod(p), y_i = a_{1i} x + a_{2i} \bmod(q)\}_{i \in \overline{L}}$
$\mathcal{U}$: send $C \longrightarrow S$.
S: accept iff the coin signature is correct,
x is correct and not repeated,
and $\forall i \in \overline{L}$, $g^{y_i} = (g^{a_{1i}})^x g^{a_{2i}} \bmod(p)$.

In the deposit protocol, the store S sends a transcript of the payment protocol to both the bank $\mathcal{B}$ and the government G.

Tracing Double Spenders
We have two coins spent:

$$C = \Pi_{i\in\overline{\mathcal{I}}}(\mathcal{H}(g^{a_{1i}} mod(p)||g^{a_{2i}} mod(p)))^{1/3}, \{x = (\mathcal{ID}_S||time)\}, \{g^{a_{1i}} mod(p), g^{a_{2i}} mod(p), y_i = a_{1i}x + a_{2i}\}_{i\in\overline{\mathcal{I}}}$$
$$C' = \Pi_{i\in\overline{\mathcal{I}}}(\mathcal{H}(g^{a_{1i}} mod(p)||g^{a_{2i}} mod(p)))^{1/3}. \{x' = (\mathcal{ID}_{S'}||time')\}, \{g^{a_{1i}} mod(p), g^{a_{2i}} mod(p), y'_i = a_{1i}x' + a_{2i}\}_{i\in\overline{\mathcal{I}}}$$

G: can solve for $\{a_{1i}, a_{2i}\}_{i\in\overline{\mathcal{I}}}$,
Compute $\mathcal{ID}_{\mathcal{U}} = Majority(\{a_{1i}a_{2i}\}_{i\in\overline{\mathcal{I}}})$

Tracing with Trustees
T_1, T_2: For the appropriate withdrawals, send $\{u_{1i}, u_{2i}\}_{i\in\overline{\mathcal{I}}}, \{v_{1i}, v_{2i}\}_{i\in\overline{\mathcal{I}}} \longrightarrow \mathcal{B}$.
G: compute supposed values $\{g^{a_{1i}}, g^{a_{2i}}\}_{i\in\overline{\mathcal{I}}}$.
For each withdrawal, try to match the supposed $\{g^{a_{1i}}g^{a_{2i}}\}_{i\in\overline{\mathcal{I}}}$ values with the supposed $\{g^{a_{1i}}g^{a_{2i}}\}_{i\in\overline{\mathcal{I}}}$ values of the deposits.
If able to match more than half the values, assume that the coin of the withdrawal is the same coin as the coin of the deposit.

We also have a protocol, **Trace-One-Payment**, which will appear in the full version of the paper.

LEMMA 3.2. *The above protocols satisfy the following properties:*

1. *They preserve the protections of [FY92] against counterfeiting and multiple spending.*
2. *We assume that finding discrete logs modulo p and inverting E_1, E_2 is hard. Then the value*

$$C = \Pi_{i\in\overline{\mathcal{I}}}(\mathcal{H}(g^{a_{1i}}\ mod(p)||g^{a_{2i}}\ mod(p)))^{1/3}\ mod(n),$$
$$\{x = (\mathcal{ID}_S||time)\},$$
$$\{g^{a_{1i}}\ mod(p), g^{a_{2i}}\ mod(p), y_i = a_{1i}x + a_{2i}\}_{i\in\overline{\mathcal{I}}}$$

appearing in the payments of a user's coins can not be linked to the values

$$\{r_i^3\mathcal{H}(g^{a_{1i}} mod(p)||g^{a_{2i}} mod(p));$$
$$E_1(u_{1i}, u_{2i}), E_2(v_{1i}, v_{2i})\}_{i=1}^k$$
$$\{(r_i, a_{1i}, a_{2i}, u_{1i}, u_{2i}, v_{1i}, v_{2i})\}_{i\in L}$$
$$\{u_{1i}, u_{2i}\}_{i\in\overline{\mathcal{I}}}\ or\ \{v_{1i}, v_{2i}\}_{i\in\overline{\mathcal{I}}}$$

appearing in the user's withdrawals (combined with the records of one trustee) by any polynomial time machine. Therefore, without help from both the trustees, the user's cash is computationly anonymous.

3. *If the user does not cheat in the withdrawal or payment protocols, then in protocols* **Trace-with-Trustees** *and* **Trace-One-Payment**, *any coin withdrawal would be linked to its payment with probability* 1.
4. *If the government is unable to find discrete logs modulo p and is unable to break $\mathcal{U}$'s signature scheme, then it is infeasible for the government (even with the help of all the trustees) to successfully claim that the user made a payment s/he did not make.*

The proof appears in the full paper.

4 The Electronic Trustee

By distributing the power to trace, the trustee-based cash systems described above are designed to improve public confidence in the privacy preservation goals of the electronic cash systems, while assuring the government that it can reliably monitor suspected criminal activity under court order. One trouble with relying solely on human trustees is that it is seemingly impossible to guard against the case where *all* the trustees misbehave and conspire with a corrupt government to trace the spending habits of honest citizens. In this section, we discuss a solution which guarantees the innocent user at least notification that s/he is being traced, even if the government and all human trustees conspire against the user.

We describe an *electronic trustee* in which both the government and the user may feel confident in placing their faith. We discuss the trustee in terms of electronic cash, but a similar trustee could be used in the context of other key-escrow systems.

For concreteness, we restrict the discussion here to the example of subsection 3.3.

The guarantees we desire for the two sides are as follows:

- The user wants to be sure that if s/he is being traced, then the user will be notified of this fact within some specified amount of time.
- The government wants to be certain that it can access each share of the user's key, as held by an electronic trustee.

Our solution requires both parties to build separately a different part of a two-part electronic trustee.

The government builds the *inner part* of the electronic trustee without knowledge of the eventual user

corresponding to the electronic trustee. This part must be *read-proof* against the user. We envision that the entire inner part may be embedded in the latest high-tech tamper-resistant material. By read-proof, we mean specifically that the user cannot alter any component of the inner part without erasing the inner part's secret signature key, Sig_T^s, and that the user cannot read the value of Sig_T^s. The government extracts the corresponding value of Sig_T^p from the inner part prior to surrendering control of the inner part to the user.

In addition to securely maintaining Sig_T^s, the inner part accepts as input the private key, Θ_T, of trustee T into a register which can be loaded exactly once by the *outer part* and is non-erasable, but readable. This is the register which the government will need to read from each electronic trustee to enable a trace of the user's spending. In order to ensure a match between the value of Θ_T, as held by the electronic trustee after installation by the user of the outer part, and the circulated value of E_T, certain precautions must be taken:
After verifying that $\Theta_T = {E_T}^{-1}$ (for the supplied or computed value of E_T), $Sig_T^s(E_T)$ is generated by the inner part, where no value $E_T{}'$, distinct from the value of E_T for which the corresponding value of Θ_T is loaded into permanent memory, will be signed. To verify that the user has placed the intact inner part inside the electronic trustee, random challenges to be signed using Sig_T^s are administered by the government, and are limited in number to the preset value in the inner part.

The outer part of the trustee, built by the user (or his/her specified vendor), monitors the output of the Sig_T^s function, and controls transmissions off the electronic trustee, in order to eliminate leakage with respect to the value of Θ_T.

In order to electronically notify the user if an attempt has been made to recover the value of Θ_T from the electronic trustee, while protecting the government from false claims of unauthorized access to Θ_T, the following procedure is specified:

The outer part generates a *pulse* key pair, $(Kpulse_T^s, Kpulse_T^p)$, where the public key $Kpulse_T^p$ is registered with a third party prior to deployment of the electronic trustee. $Kpulse_T^s$ is used to sign periodic sequenced messages (verifiable using $Kpulse_T^p$) which effectively affirm that no attempt has been made to retrieve Θ_T, since the user can implement the outer part so that $Kpulse_T^s$ is automatically erased upon intrusion of the electronic trustee. After the government is satisfied that nothing has been introduced into the outer part which can later obliterate Θ_T from the retrievable memory of the inner part, the electronic trustee is coated (under user and government supervision). It is in the user's (legitimate) interest to apply a coating which alters upon tampering, and is impossible to reproduce exactly, or to predetermine. The government assures itself that the outer part and the coating are constructed so that the coating can't be modified spontaneously or from within. A digitization of the coating is signed by the outer part's $Kpulse_T^s$ key, where the user can design and implement the $Kpulse_T^s$ function so as to thereafter accept only internally generated inputs. Alternatively, the digitized value of the coating is (physically) signed by the user or his/her legal representative. The signed version of the coating value is supplied to the government. The electronic trustee is, from then on, held securely under government control.

5 Adding Anonymous Change-making

We address the problem of the user $\mathcal{U}$ wishing to make an anonymous purchase from a store $\mathcal{S}$ but having incorrect change. We assume that the store has a computer link to a bank $\mathcal{B}$ but that the user does not wish to identify him/herself to the bank to prevent the bank from associating him or her with the store. We assume that the user has Y dollars in coins and wishes to make a purchase worth $X < Y$ dollars.

We present a protocol which allows a user $\mathcal{U}$ to present anonymously a set of coins worth Y dollars to the bank $\mathcal{B}$ and receive in return another set of coins also worth Y dollars, but in different denominations. The user chooses the denominations in such a way that the he or she can combine coins to get X dollars.

Getting Anonymous Change

$\mathcal{U}$ wishes to give $\mathcal{B}$ Y dollars in coins and receive Y dollars in coins of different denominations.

$\mathcal{U}$: use the payment protocol to pay the Y dollars in coins to bank $\mathcal{B}$ (without revealing $\mathcal{ID}_\mathcal{U}$) and tell $\mathcal{B}$ the desired denominations of the change.

$\mathcal{B}$: check that the requested coins total Y dollars. Let m'_{old} be a value from one of the coins that $\mathcal{U}$ just paid. For every coin to be given out as change, $\mathcal{B}$ uses the appropriate value of h_i.

For complete anonymity, $\mathcal{B}$ and $\mathcal{U}$ use value $m_{new} = m'_{old}$ for each new coin withdrawn.

For trustee-based tracing, $\mathcal{U}$ generates a new value $f_{new} = g_3^{\gamma_3} g_4^{\gamma_4}$ for each new coin and sends the trustees shares of γ_3, γ_4. $\mathcal{U}$ and $\mathcal{B}$ use value $m_{new} = m'_{old} f_{new}$ in the withdrawal of that coin.

LEMMA 5.1. *The above protocol, when added to either Brands' basic protocols or to the trustee-based system of subsection 3.2, maintains the following properties:*

1. *The augmented system is secure against user counterfeiting and multiple spending.*

2. *Without help from all the trustees, the values appearing in the payments of a user's coins are completely independent from the values appearing in the user's withdrawals.*

3. *If we use the trustee-based system of subsection 3.2, then the trustees can combine their information and trace both the user's original coins and the coins given as change.*

See Appendix A for the proof.

6 Conclusions and Open Problems

In this extended abstract, we have addressed several important issues for an electronic cash system. We have presented the outline of a system which is feasible, secure against criminal attack, and still largely acceptable to users who are concerned about excessive invasion of their privacy. The system which we haved proposed has the benefits of previously proposed electronic cash systems as well as other benefits, including the prevention of certain types of crime, and an efficient, privacy-maintaining solution of the anonymous change problem.

One topic which deserves further investigation is the anonymous change problem. In this extended abstract, we presented a way in which a user might make an anonymous $1 purchase with a $2 coin at a store that has a line of communication to a minting facility. However, if the store does not have this communication capability, the problem remains open. The solutions of [OO92] and [EO94] come close, but the parts of the divisible coin are linkable. We argued in this extended abstract that any off-line, unlinkable solution must base the user's anonymity on complexity assumptions. [W92] discusses a way it could be done using zero-knowledge proofs, but these proofs may not be feasible for the user to carry out in practice.

References

[B93] S. Brands. Electronic Cash Systems Based on the Representation Problem in Groups of Prime Order. Preproceedings of CRYPTO 93.

[B93b] S. Brands. Untraceable Off-line Cash in Wallets with Observers. Proceedings of CRYPTO 93, pp 302- 318.

[Btr93] S. Brands. An Efficient Off-line Electronic Cash Systems Based on the Representation Problem. C.W.I. Technical Report CS-T9323, The Netherlands.

[Cha83] D. Chaum. Blind Signatures for Untraceable Payments. Advances in Cryptology - Proceedings of CRYPTO 82, 1983, pp199-203.

[Cha84] D. Chaum. Blind Signature Systems. Advances in Cryptology - Proceedings of CRYPTO 83, 1984.

[Cha85] D. Chaum. Security Without Identification: Transaction Systems to Make Big Brother Obsolete. Comm. ACM 28, 10 (October 1985).

[Cha88] D. Chaum. Privacy Protected Payments: Unconditional Payer And/Or Payee Untraceability. Smartcard 2000, North Holland, 1988.

[Cha89] D. Chaum. OnLine Cash Checks EuroCrypt 89 pp 288- 293.

[CFN90] D. Chaum, A. Fiat, M. Naor. Untraceable Electronic Cash. Advances in Cryptology - Proceedings of CRYPTO 88, pp319-327.

[CP92] D. Chaum, T.P. Pedersen Transferred Cash Grows in Size Eurocrypt 92

[CP93] D. Chaum, T.P. Pedersen. Wallet databases with Observers Advances in Cryptology - Proceedings of CRYPTO 92, 1993.

[EO94] T. Eng, T. Okamoto. Single-Term Divisible Electronic Coins Preproceedings of Eurocrypt 94, pp 311-325.

[FY92] M. Franklin, M. Yung Towards Provably Secure Efficient Electronic Cash Columbia Univ. Dept of C.S. TR CUCS-018-92, April 24, 1992.

[OO90] T. Okamoto, K. Ohta. Disposable Zero-Knowledge Authentication and Their Applications to Untraceable Electronic Cash Advances in Cryptology - Proceedings of CRYPTO 89, 1990, pp481-496.

[OO92] T. Okamoto, K. Ohta. Universal Electronic Cash Advances in Cryptology - Proceedings of CRYPTO 91, 1992, pp324-337.

[vA90] H. van Antwerpen. Electronic Cash. Master's thesis, CWI, 1990.

[vSN92] S. von Solms and D. Naccache. On Blind Signatures and Perfect Crimes. Computers and Security, 11 (1992) pp581-583.

[W92] D. Wilson. Cash Subdividable into Unlinkable Pieces. Unpublished manuscript.

Appendix A: Proofs

Proof. (of lemma 3.1) (sketch)

The new protocols satisfy the following properties:

1. The form of the bank's blind signature has not been altered and the bank reveals no more information than it did in Brands' basic protocols. Therefore, the proof of proposition 7 of [B93b] goes through, and, assuming that it is infeasible to existentially forge Schnorr signatures, the new system is secure against counterfeiting.

   The proof relating to the traceability of multiple spenders goes through as it does for Brands' original protocols. The only difference is that now we assume that the user is unable to find a non-trivial representation of 1 relative to generators

g_1, g_2, g_3, g_4, g. If $\mathcal{U}$ spends a coin twice, the bank will be able to deduce the value of s corresponding to that coin and use that value to deduce $u_1, u_2, I_{\mathcal{U}} = g_1^{u_1} g_2^{u_2}$.

2. The proof of this statement is similar to the proof of the corresponding statement for Brands' basic protocols (see [Btr93]).

3. Proof to appear in the full paper.

4. Proof to appear in the full paper.

5. Suppose G mistakenly identifies user $\hat{I}$'s money as I's. Let $\hat{d}$ be the denomination of $\hat{I}$'s coin. Let $\hat{f}_{\hat{k}} = g_3^{\hat{\gamma}_{3,k}} g_4^{\hat{\gamma}_{4,k}}$ be $\hat{I}$'s random value. Let $\hat{s}$ be the first random value which $\hat{I}$ chose for the coin in the withdrawal protocol. Let $\hat{u}_1, \hat{u}_2$ be the exponents in $\hat{I}$'s known representation.

   Then:

$$I_{\hat{\mathcal{U}}} d\hat{f}_{\hat{k}} = (m'^{r_3^{-1}})^{\hat{\gamma}_{3,\hat{k}}}$$

$$= (((I_{\mathcal{U}} df_k)^s)^{(\gamma_{3,k}s)^{-1}})^{\hat{\gamma}_{3,\hat{k}}} = (I_{\mathcal{U}} df_k)^{\gamma_{3,k}^{-1}\hat{\gamma}_{3,\hat{k}}}$$

   So

$$g_1^{\hat{u}_1} g_2^{\hat{u}_2} g_3^{\hat{\gamma}_{3,\hat{k}}} g_4^{\hat{\gamma}_{4,\hat{k}}} d$$

$$= g_1^{u_1\gamma_{3,k}^{-1}\hat{\gamma}_{3,\hat{k}}} g_2^{u_2\gamma_{3,k}^{-1}\hat{\gamma}_{3,\hat{k}}} g_3^{\gamma_{3,k}\gamma_{3,k}^{-1}\hat{\gamma}_{3,\hat{k}}} g_4^{\gamma_{4,k}\gamma_{3,k}^{-1}\hat{\gamma}_{3,\hat{k}}} d^{\gamma_{3,k}^{-1}\hat{\gamma}_{3,\hat{k}}}$$

   This yields the following representation of 1:

$$\left(\frac{\hat{\gamma}_{3,\hat{k}} u_1}{\gamma_{3,k}} - \hat{u}_1, \frac{\hat{\gamma}_{3,\hat{k}} u_2}{\gamma_{3,k}} - \hat{u}_2, 0, \frac{\gamma_{4,k}\hat{\gamma}_{3,\hat{k}}}{\gamma_{3,k}} - \hat{\gamma}_{4,\hat{k}}, \frac{\hat{\gamma}_{3,\hat{k}}}{\gamma_{3,k}} - 1\right)$$

   This representation is non-trivial if $\gamma_{3,k} \neq \hat{\gamma}_{3,\hat{k}}$ or $\gamma_{4,k} \neq \hat{\gamma}_{4,\hat{k}}$ or $u_1 \neq \hat{u}_1$ or $u_2 \neq \hat{u}_2$. For distinct users, the bank will demand that $I_{\mathcal{U}} \neq I_{\hat{\mathcal{U}}}$. If $\mathcal{U} = \hat{\mathcal{U}}$, the bank will demand that $f_k \neq \hat{f}_{\hat{k}}$, ie for a given user, the bank will demand that all the f_k values are distinct.

Proof. (of lemma 5.1)

1. Without loss of generality, we assume that we are augmenting a trustee-based system. The completely anonymous system is simpler.

   We divide the user's coins up into the *old* coins (Y dollars worth) given by the user to the bank and the *new* coins (Y dollars worth) given in return by the bank to the user.

   We can assume that the user can not feasibly double-spend the old coins. This is so because we already know that the user can not double-spend coins s/he will withdraw using the regular withdrawal protocol and we will also show that s/he can not double-spend the new coins.

   Let the following coin withdrawal and payment values correspond to an old coin used to form the new coins. We assume at first that the old coin is withdrawn using the **Withdrawal-With-Trustees** protocol where $\mathcal{U}$ proves his/her identity to $\mathcal{B}$.

$$f_k, m = I_{\mathcal{U}} df_k, s, m' = m^s = (I_{\mathcal{U}} df_k)^s$$

   We consider the following new coin with values:

$$f^{new}, s^{new}, m^{new} = m'_{old} f^{new} = (I_{\mathcal{U}} df_k)^s f^{new}$$

$$m^{new\prime} = (m^{new})^{s^{new}} = ((I_{\mathcal{U}} df_k)^s f^{new})^{s^{new}}$$

   $\mathcal{U}$'s representation of $m^{new\prime}$ is $m'_n =$

$$g_1^{u_1 s s^{new}} g_2^{u_2 s s^{new}} g_3^{(\gamma_{3,k}s + \gamma_3^{new})s^{new}} g_4^{(\gamma_{4,k}s + \gamma_4^{new})s^{new}} d^{s s^{new}}$$

   If $\mathcal{U}$ does spend the new coin more than once, then s/he will reveal the value ss^{new} and the bank can deduce $u_1, u_2, I_{\mathcal{U}} = g_1^{u_1} g_2^{u_2}$. Therefore, $\mathcal{U}$ can not effectively double-spend the new coin.

   If the old coin was itself a coin obtained from the anonymous change protocol, then the user's knowledge of the new coin will have the form:

$$m'_n = g_1^{u_1(\Pi_j s_j)} g_2^{u_2(\Pi_j s_j)} g_3^{\delta_3} g_4^{\delta_4} d^{(\Pi_j s_j)}$$

   where the values $\{s_j\}_j$ are from the original withdrawal and the times the user obtained anonymous change and the values δ_3, δ_4 are computed by the user.

   If $\mathcal{U}$ double-spent this coin, $\mathcal{B}$ could deduce $(\Pi_j s_j), u_1, u_2, I_{\mathcal{U}}$.

2. This proof is similar to those for the corresponding statements for Brands' basic system and for the system presented in subsection 3.2.

3. To answer the question of whether $\mathcal{U}$ made a particular payment, the trustees trace the user's original withdrawals (when the user proved his/her identity to the bank) to the executions of the anonymous change protocols. Then the trustees trace the new coins from the anonymous change protocols using the value $\gamma_{3,k}s + \gamma_3^{new}$.